UNITED STATES DISTRICT COURT
DISTRICT OF NEW HAMPSHIRE

IN THE MATTER OF THE SEARCH OF THE PREMISES OF STORAGE UNIT E9 OF "603 STORAGE" LOCATED AT 131 BURKE STREET IN NASHUA, NEW HAMPSHIRE	No. 21-mj-297-AJ-01

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Ryan S. Burke, depose and state as follows:

AGENT BACKGROUND

1. I am a Special Agent of the Federal Bureau of Investigation ("FBI") and have been so employed since October 2012. I am currently assigned to the FBI's New Hampshire Safe Streets Gang Task Force ("SSGTF") where I am tasked with investigating gang members, violent criminals, and major offenders throughout the state. As part of the SSGTF, I work alongside law enforcement officers from various local, state, and federal agencies throughout the state of New Hampshire.

2. I am an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code, and am empowered by law to conduct investigations of and to make arrests for offenses enumerated in Section 2516 of Title 18, United States Code. I also am a "federal law enforcement officer" within the meaning of Rule 41 of the Federal Rules of Criminal Procedure.

3. Throughout my career, I have led and/or been involved with investigations of robberies, kidnappings, murders, fugitives, extortions, threats, drug distribution, illegal possession of firearms, and other crimes. My investigations have included the use of the following investigative techniques: physical surveillance; handling of cooperating sources and witnesses;

exploitation of cellular, social media, and Internet Protocol ("IP") based communications data; execution of search and seizure warrants; wire, electronic, and oral wiretaps; and the execution of arrest warrants.

4. Based on my training, experience, and information provided to me by other law enforcement officers, I am familiar with the modus operandi used by individuals engaged in the violation of various criminal offenses, such as those related to acts of violence, firearms, and controlled substances. For example, I have handled many cooperating sources and witnesses who have provided information to me specifically related to shootings, the distribution of controlled substances, and various firearms offenses. I have also reviewed thousands of court-authorized wiretap intercepts between drug traffickers, violators of firearm offenses, individuals conspiring to commit armed robberies, and individuals engaged in the violation of other offenses. Many of these investigations have resulted in the execution of search warrants, arrest warrants, and eventual convictions.

PURPOSE OF AFFIDAVIT

5. I submit this affidavit in support of an application for a warrant to search the following premises:

a. Storage Unit E9 of "603 Storage" located at in Nashua, New Hampshire (hereafter, the "**Target Premises**").

6. Based on the information contained herein, there is probable cause to believe that **Target Premises**, described in Attachment A, contains evidence, fruits, and instrumentalities as further described in Attachment B of the crimes of 21 U.S.C. § 841(a)(1) [Possession with the Intent to Distribute and the Unlawful Distribution of Controlled Substances].

7. The information set forth in this affidavit is based on my personal participation in this investigation, as well as my training and experience, and information received from other law

enforcement officers. I have not set forth every detail I or other law enforcement officers know about this investigation but have set forth facts that I believe are sufficient to evaluate probable cause as it relates to the issuance of the requested warrant.

PROBABLE CAUSE

8. On November 16, 2021, the Honorable United States Magistrate Judge Andrea K. Johnstone (District of New Hampshire) authorized a warrant to arrest Matthew Espersen (YOB: 1985) for violations of 21 U.S.C. §§ 841(a)(1) and (b)(1)(C) – Possession with Intent to Distribute Controlled Substances, specifically, fentanyl and methamphetamine.

9. On November 22, 2021, law enforcement conducted surveillance outside of the **Target Premises** in order to effect Espersen's arrest upon his arrival. The **Target Premises** had been previously identified by law enforcement as a place frequented by Espersen[1] and thus became the center of law enforcement's arrest efforts. That evening, Espersen was observed driving his black BMW 328i sedan (bearing New Hampshire license plate to 603 Storage; inputting the key code to enter the secured storage facility; and then parking in front of the **Target Premises**. After exiting his vehicle, Espersen utilized a key to open the **Target Premises** and entered. Another individual (hereafter, "CW-1") then approached on foot and joined Espersen inside the **Target Premises**.

10. With Espersen and CW-1 inside the **Target Premises**, law enforcement approached and effected Espersen's arrest from inside the **Target Premises**. CW-1 was detained and questioned. During questioning, CW-1 agreed to let law enforcement search his backpack. Upon doing so, law enforcement located a black eyeglass case which contained a small quantity of suspected heroin/fentanyl. CW-1 then informed law enforcement that he contacted Espersen by

[1] Espersen had been observed multiple times by law enforcement at the **Target Premises** in the month of November 2021.

telephone prior to his arrival at the **Target Premises** for the purpose of obtaining "dope" from Espersen. Based on my training and experience, I understood "dope" to be street slang for heroin/fentanyl. CW-1 further stated that immediately upon his arrival, he walked into the **Target Premises** and received the black eyeglass case from Espersen. CW-1 informed law enforcement that he has obtained controlled substances from Espersen in the past.

12. Based on the statements made by CW-1 and the observations made by law enforcement from outside of the **Target Premises**, I believe the **Target Premises** contains controlled substances and other items commonly used by individuals engaged in the distribution of controlled substances. Furthermore, I believe these items were under the control of Espersen who possessed the key to the **Target Premises** on his keychain.

Training and Experience Concerning Items to be Seized

13. Based upon my training and experience, as well as the collective knowledge and experience of other agents and police officers in my office, I am aware that drug traffickers very often store controlled substances, firearms, and other tools of the drug trade in their homes, automobiles, garages or outbuildings on their properties, basements, or other places under their immediate control. I am aware that it is generally a common practice for drug traffickers to store their drug inventory and drug-related paraphernalia including, but not limited to, scales, plastic baggies, wrapping material, paper or plastic bundles, and zip lock bags, in residences or other locations they access with frequency. Based on my training and experience, powder drugs such as fentanyl are generally brought into the region in bulk. However, such drugs are not typically consumed by users in such high purity form. Rather, such powder drugs, when ultimately consumed by the user, are at a lower purity level. High purity powder drugs are reduced in purity by the addition of dilutants. This process is called "cutting" or "stepping on" the drug. Other equipment, such as scales, presses, grinders, razor blades, glass panes, blenders, and mirrors, and the like are typically used in this cutting process. Once the drug has been "cut," a usual practice is to repackage or “press” it in smaller quantities such as ten (10) gram fingers or other types of plastic bags for redistribution.

14. It is generally a common practice for drug traffickers to maintain in hard copy or on other electronic devices, records relating to their drug trafficking activities. Because drug traffickers in many instances will "front" (that is, sell on consignment) controlled substances to their clients, or alternatively, will be "fronted" controlled substances from their suppliers, such record-keeping is necessary to keep track of amounts paid and owed, and such records will also be maintained close at hand so as to readily ascertain current balances.

15. Drug traffickers will commonly maintain records and documents which provide a paper trail for money laundering of illicit drug trafficking proceeds, often long after the actual transactions. There are many reasons why an individual will generally maintain records for long periods of time. One reason is that the records will often seem innocuous because of their nature (e.g. financial, credit card and banking documents, travel documents, receipts, client lists, documents reflecting purchases of assets, personal calendars, telephone and address directories, check books, videotapes and photographs, utility records, ownership records, letters and notes, tax returns and financial records, escrow files, telephone bills, keys to safe deposit boxes, packaging materials, computer hardware and software). Second, the individual may no longer realize he/she still possesses the records or may believe law enforcement could not obtain a search warrant to seize the evidence. Lastly, it is common for individuals to set aside or store such records, and because they generally have no immediate need for the records, they are often forgotten. To law enforcement, however, all these items may have significance and relevance when considered in light of other evidence.

16. Additionally, drug traffickers must maintain telephone and address listings of clients and suppliers and keep them immediately available in order to efficiently conduct their drug trafficking business. Drug traffickers may also keep lists of customers, the cars they drive, and the

phones they use in order to keep track of them. They may also collect court papers and other documents about customers who they believe may be cooperating with law enforcement authorities in order to protect themselves or attempt to intimidate potential cooperators.

17. It is also a generally common practice for traffickers to conceal at their residences, or other places they access frequently, large sums of money, either the proceeds from drug sales or monies to be used to purchase controlled substances. Individuals who distribute controlled substances often use cash or readily transported assets which are used as cash equivalents like pre-paid debit cards, gift cards, bearer bonds, gold, diamonds, or jewels because of the illegal nature of the transactions and to lessen the possibility of a financial paper trail. Additionally, drug traffickers typically make use of wire transfers, cashier's checks, and money orders to pay for controlled substances. They may also use banks and wire companies, both foreign or domestic, to launder and transfer funds to co-conspirators. They may also use shipping companies and keep records of shipments of goods bought with drug proceeds. Records relating to income and expenditures of money and wealth in connection with drug trafficking would also typically be maintained in residences. I know that drug traffickers sometimes purchase real estate with suspected drug proceeds. They may keep records of real estate transactions, money received from rental properties, and other such documents in their residences.

18. Based on my training and experience, I know that individuals involved in the distribution of controlled substances attempt to hide the true identity of their residence and, further, employ methods of surveillance at such residence in order to evade law enforcement. Typically, these individuals will maintain at their residence documents relating to the identity of the person(s) in residence, occupancy, control, or ownership of the subject premises. Such identification evidence is typical of the articles people commonly maintain in their residences, such as canceled

mail, deeds, leases, rental agreements, photographs, personal telephone books, diaries, utility and telephone bills, statements, identification documents, and keys. I know that drug traffickers often use storage units to store drug proceeds and that keys or records of these units may be kept in residences.

19. Often, drug traffickers possess firearms and other dangerous weapons to protect their profits, supply of drugs, and persons from others who might attempt to forcibly take the traffickers' profits and/or supply of drugs.

20. Based on my training and experience, I know that drug traffickers typically use cellular telephones in order to facilitate drug transactions, including to order and take orders for controlled substances or to set up shipments. I am aware that items such as cell phones and U.S. currency are often located in a residence or on an individual's person.

21. Individuals involved in the illicit distribution of controlled substances often take or cause to be taken photographs of themselves, their associates, their property and their product and such items are usually maintained within their residence and sometimes on cell phones.

22. It is common for individuals who are involved in the trafficking and distribution of controlled substances to store the records of those activities and proceeds of those activities in secure areas over which they have control such as safes, bags, locked drawers, briefcases, and duffel bags, among other locked containers.

23. I know that individuals who distribute narcotics often utilize motor vehicles in order to obtain quantities of controlled substances from their source of supply for distribution. I also know that individuals who are engaged in the distribution of controlled substances utilize motor vehicles in order to transport controlled substances to various locations in order to meet with and distribute controlled substances to potential drug purchasers.

Training and Experience on Digital Devices

24. In addition to documentary evidence of financial and drug trafficking crimes, drug traffickers commonly possess and use multiple cellular telephones simultaneously to conduct their drug trafficking activities and many of these cellular telephones are kept at drug stash houses or at the dealers' own residences. It is common for these cellular telephones to be retained, although not necessarily used, for months or longer by drug traffickers in their vehicles, residences, and businesses. Drug traffickers often do not discard their cellular telephones immediately after they stop actively using them. Therefore, while it is common for drug traffickers to stop using cellular telephones frequently, it is far less common for drug traffickers to discard their cellular telephones after they switch to new cellular telephones. I am aware that collections of cell phones have been found during drug trafficking search warrants of stash houses or residences that have included cell phones that were no longer being used by a particular drug trafficker but had nevertheless been retained.

25. As noted above, evidence of drug crimes can be found in the cell phones and smart phones referenced in the preceding paragraphs. Such evidence can include internet searches for drug-related paraphernalia, addresses, or telephone numbers, as well as incriminating communications via emails, text messages or instant messages. Actions such as internet searching or emailing (in addition to calling) and text messaging can now be performed from most cell phones. I know, based on my training and experience, that drug traffickers may use encrypted chat platforms like Whatsapp, Textnow, Facebook Messenger, and Instagram, to communicate with people in other countries (often countries from where drugs are brought into the United States) and with people who are most cautious about law enforcement detection. Other applications like

Venmo or Cashapp allow people to quickly make financial transfers to others and drug customers may use these methods to pay their sources of supply for drugs.

26. In addition, those involved in drug trafficking crimes commonly communicate using multiple cellular telephones. Contemporaneous possession of multiple cellular telephones is, therefore, evidence of drug trafficking. Moreover, the particular numbers of and the particular numbers dialed by particular cellular telephones can be evidence of drug trafficking. Such numbers can confirm identities of particular speakers and the occurrence of certain events. Based on my training, experience, and information provided by other law enforcement officers, I know that many smartphones can now function essentially as small computers. Smartphones have capabilities that include serving as a wireless telephone, digital camera, portable media player, GPS navigation device, sending and receiving text messages and e-mails, and storing a vast range and amount of electronic data. Examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

27. As with most electronic/digital technology items, communications made from an electronic device, such as a computer or a cell phone, are often saved or stored on the device. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that data in digital form can be stored on a variety of digital devices and that during the search of a premises it is not always possible to search digital devices for digital data for a number of reasons, including the following:

a. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of digital devices and software programs in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized

equipment necessary to conduct a thorough search. In addition, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.

c. The volume of data stored on many digital devices will typically be so large that it will be highly impractical to search for data during the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 500 or more gigabytes are now commonplace. Consequently, just one device might contain the equivalent of 250 million pages of data, which, if printed out, would completely fill three 35' x 35' x 10' rooms to the ceiling. Further, a 500 gigabyte drive could contain as many as approximately 450 full run movies or 450,000 songs.

d. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed

via the Internet. Electronic files saved to a hard drive can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, i.e., space on a hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space, for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files that have been viewed on the Internet are often automatically downloaded into a temporary directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently downloaded or viewed content. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Recovery of residue of electronic files from a hard drive requires specialized tools and a controlled laboratory environment. Recovery also can require substantial time.

e. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processing, picture, and movie files), digital devices can contain other forms of electronic evidence as

well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications and materials contained on the digital devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive image as a whole. Digital data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

f. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data on a digital device is not segregable from the digital device. Analysis of the digital device as a whole to demonstrate the absence of particular data requires specialized tools and a controlled laboratory environment and can require substantial time. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

28. Based on my training and experience, I believe that it is likely that the **Target Premises** will contain smartphones that can be unlocked via the use of a fingerprint or facial recognition in lieu of a numeric or alphanumeric password. I know from my training and experience, as well as from information found in publicly available materials including those published by Apple, that some models of devices such as iPhones and iPads, offer their users the ability to unlock the device via the use of a fingerprint or facial recognition in lieu of a numeric or alphanumeric passcode or password. This feature is called Touch ID.

29. If a user enables Touch ID or facial recognition on a given device, he or she can register numerous fingerprints or facial profiles that can be used to unlock that device. The user can then use any of the registered fingerprints or facial profiles to unlock the device by pressing

the relevant finger(s) to the device's Touch ID sensor or by looking into the device's camera. In my training and experience, users of Apple devices that offer Touch ID or facial recognition often enable it because it is considered to be a more convenient way to unlock the device than by entering a passcode, as well as a more secure way to protect the device's contents. This is particularly true when the user(s) of the device are engaged in criminal activities and thus have a heightened concern about securing the contents of the device.

30. In some circumstances, a fingerprint cannot be used to unlock a device that has Touch ID or facial recognition enabled, and a passcode must be used instead, such as: (1) when a certain amount of time has passed since the last time the device was unlocked and (2) when the device has not been unlocked via Touch ID or facial recognition recently and the passcode or password has not been entered in the last few days. Thus, in the event law enforcement encounters a locked Apple device, the opportunity to unlock the device via Touch ID or facial recognition exists only for a short time.

31. Although Apple's Touch ID or facial recognition may be the most common or well-known means for unlocking a device with a fingerprint or facial profile, I am aware that other brands of smartphones like Samsung also offer similar features that work essentially in the same way. Therefore, when I refer to Touch ID or facial recognition I am not just referring to Apple devices, but to similar technology on all smartphones. While I believe that the targets of this investigation likely use smartphones, I am not aware of the particular brand of phone that they use.

32. The passcodes that would unlock the targets' devices is not known to law enforcement. Thus, it may be necessary to press the fingers of the user of the device to the device's Touch ID sensor or put the device's camera in front of the user's face in an attempt to unlock the device for the purpose of executing the search authorized by this warrant. Attempting to unlock

devices with the use of the fingerprints or facial profile of the user is necessary because the government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant.

CONCLUSION

33. For all the reasons described above, I submit that there is probable cause to believe that evidence and fruits of the violations of 21 U.S.C. § 841(a)(1) [Possession with the Intent to Distribute and the Unlawful Distribution of Controlled Substances], will be found by searching the premises described in Attachment A. Based upon my training and experience I believe that the items set forth in Attachment B are commonly possessed by drug traffickers in their storage units, on their cell phones, or in other places under their control and that those items are evidence of violations of the offenses being committed by Espersen. Additionally, I believe that there are dangerous drugs inside the **target premises** in plain view that are a danger to the area surrounding the unit. It is unknown if other individuals have access to the **target premises** and could remove items from the storage unit. For these reasons, I request that we be allowed to search the premises at any time of the day or night.

/s/ Ryan S. Burke
Ryan S. Burke, Special Agent
Federal Bureau of Investigation

The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. Crim. P. 4.1 and affirmed under oath the content of this affidavit and application.

Date: Nov 22, 2021
Time: 7:54 PM, Nov 22, 2021

HONORABLE ANDREA K. JOHNSTONE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be Searched

Storage Unit E9 of "603 Storage" located at 131 Burke Street in Nashua, New Hampshire (hereafter, the "Target Premises").

ATTACHMENT B

Items to be Seized

1. All records, in whatever form, and tangible objects that constitute evidence, fruits, or instrumentalities of violations of 21 U.S.C. § 841 [Possession with the Intent to Distribute and the Unlawful Distribution of Controlled Substances] by Matthew Espersen and any co-conspirators, including information and items related to:

   a. Controlled substances and materials consistent with controlled substances packaging;

   b. United States currency, foreign currencies, and other forms of currency acquired or used during transactions involving contraband;

   c. Weapons to include handguns, ammunition, rifles, shotguns, hand crafted guns, explosive devices, etc., in which there is no immediate appearance of legitimate use and of which may be used in conjunction with the distribution of controlled substances;

   d. Places and locations where evidence of the above-referenced criminal offenses was obtained or discarded, or is currently stored;

   e. The identities of any co-conspirators, as well as any co-conspirators' acts taken in furtherance of the offenses enumerated in this application;

   f. Electronic devices, including mobile electronic equipment, serial numbers or any electronic identifiers that serve to identify the equipment, and the information stored electronically on the devices, specifically:

      i. telephone logs, contact lists, other records reflecting names, aliases, addresses, telephone numbers, and other contact or identification data;

      ii. the actual and attempted possession, purchase, receipt, sale, pawn, trade, transfer, transportation, shipment, or other disposition of controlled substances, including buyer lists, seller lists, notes, pay-owe sheets, records of sales, logs, receipts, and communications;

      iii. the actual and attempted possession, purchase, receipt, sale, pawn, trade, transfer, transportation, shipment, or other disposition of firearms and ammunition, including buyer lists, seller lists, notes, pay-owe sheets, records of sales, logs, receipts, and communications;

      iv. messages and other communications related to controlled substances and firearms violations and activity;

v. photographs, images, and depictions of controlled substances, firearms, and currency;

vi. who used, owned or controlled the equipment;

vii. when the equipment was used;

viii. the travel and whereabouts of the user of the equipment;

ix. the attachment of other hardware or storage media;

x. the use of counter-forensic programs and associated data that are designed to eliminate data;

xi. passwords, encryption keys, and other access devices that may be necessary to use the equipment; and

xii. accounts associated with software services or services providing Internet access or remote storage of either data or storage media

2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. Items described in Paragraph 1(a) through (i);

b. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

c. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

d. evidence of the lack of such malicious software;

e. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

f. evidence indicating the computer user's state of mind as it relates to the crimes under investigation;

g. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

h. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

i. evidence of the times the COMPUTER was used;

j. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

k. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

l. records of or information about Internet Protocol addresses used by the COMPUTER;

m. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

n. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

During the execution of the search of the property described in Attachment A, law enforcement officers are authorized to press or swipe the fingers (including thumbs) of any individual, who is found at the subject Target Premises and reasonably believed by law enforcement to be a user of the device, to the fingerprint scanner of the device; and/or (2) hold the device in front of the face of those same individuals and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search its contents as authorized by this warrant.